PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference MRB.P53007WO	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP2004/050129	International filing date *(day/month/year)* 13.02.2004	Priority date *(day/month/year)* 13.02.2004
International Patent Classification (IPC) or both national classification and IPC INV. H04L12/56 H04L29/08 H04L29/12 H04L29/06		
Applicant OY LM ERICSSON AB et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 10 sheets.

3. This report contains indications relating to the following items:

I ☒ Basis of the opinion
II ☐ Priority
III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
IV ☐ Lack of unity of invention
V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
VI ☐ Certain documents cited
VII ☐ Certain defects in the international application
VIII ☐ Certain observations on the international application

Date of submission of the demand 07.12.2005	Date of completion of this report 08.05.2006
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Bengi-Akyuerek, K Telephone No. +49 89 2399-7105

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-10, 15-21	as originally filed
11-14, 14a	received on 08.12.2005 with letter of 07.12.2005

Claims, Numbers

1-26	received on 08.12.2005 with letter of 07.12.2005

Drawings, Sheets

1/11-11/11	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

□ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

□ the language of publication of the international application (under Rule 48.3(b)).

□ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

□ contained in the international application in written form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readable form.

□ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

□ the description, pages:

□ the claims, Nos.:

□ the drawings, sheets:

5. □ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-26
	No:	Claims	-
Inventive step (IS)	Yes:	Claims	1-26
	No:	Claims	-
Industrial applicability (IA)	Yes:	Claims	1-26
	No:	Claims	-

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Article 35(2) PCT with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following documents cited in the International Search Report are referred to in this communication:

D1: EGGERT L: "Host Identity Protocol (HIP) Rendezvous Mechanisms; draft-eggert-hip-rendezvous", 5 February 2004 (2004-02-05), XP002300905

D2: NIKANDER P ET AL: "End-Host Mobility and Multi-Homing with Host Identity Protocol; draft-nikander-hip-mm-00.txt", 17 June 2003 (2003-06-17), XP015004615

2 The present invention relates to methods (**claims 1 and 20**), an associated system (**claim 19**), and an associated apparatus (**claim 21**) for managing HIP-based connections between legacy (i.e., non-HIP enabled) and HIP-enabled nodes.

3 The subject-matter of the present application appears to be novel and inventive over the cited prior art (Article 33(2) and (3) PCT) and therefore meets the criteria mentioned in Article 33(1) PCT:

3.1 Document **D1**, which is considered as closest prior art, discloses with regard to the broadest **claim 20** (the references in parentheses applying to this document):

A method of use by an HIP proxy ("DNS"; Fig. 4) of partially securing communications, via the HIP proxy, between a first host ("non-HIP Initiator"; Fig. 4), which is not HIP-enabled and a second host ("HIP Responder"; Fig. 4), which is HIP-enabled, comprising the steps of:

(a) receiving a query ("FQDN(R)") from the first host to resolve the IP address of the second host (Fig. 4, step #3);

(b) in response to said query, retrieving an IP address ("IP(RVS)") and an HIT ("HI(R)") associated with the second host (Fig. 4, step #4);

(c) maintaining a mapping between the retrieved IP address ("IP(RVS)") and the retrieved HIT ("HI(R)");

(d) using the mapping to negotiate a HIP connection between a Rendezvous Server and the second host, upon receipt of a session initiation message at the Rendezvous Server from the first host including the IP address ("IP(RVS)") as its destination address (page 9, section 4.1, first paragraph: "...a non-HIP initiator starts communication with a HIP node"; page 9, section 4.1, last paragraph: "...non-HIP node I...sets up transport-layer connections using the IP addresses IP(RVS)..."; Fig. 4, step #5).

3.2 As a result, the subject-matter of **claim 20** differs from that of document **D1** in that, in response to said retrieval of an IP address and an HIT, a substitute IP address associated with the second host is returned by the HIP proxy and that the HIP proxy itself is responsible for controlling the HIP connections.

3.3 Therefore, the objective problem underlying **claim 20** is regarded as how to centrally control HIP connections between legacy and HIP-enabled nodes located behind an intermediary forwarding node.

3.4 In view of the teachings of document **D1**, the person skilled in the art would not arrive at the proposed solution to the above-mentioned problem since in **D1** the the DNS and the Rendezvous Server are not connected to each, hence the actual HIP proxy, i.e., the Rendezvous Server, may not centrally control the establishment of HIP connections in the presence of another intermediary (forwarding) node.

3.5 Equally, document **D2** neither alone nor in combination with **D1** discloses or suggests the subject-matter of **claim 20** since it is merely related to standard readressing mechanisms in generic HIP-based connections including Forwarding Agents.

4 In the light of the above-mentioned reasons regarding independent method **claim 20**, the subject-matter of independent **claims 1, 19, and 21** is also considered novel and inventive, since it is directed to corresponding complementary units.

It is desirable to provide a method of at least partially securing communications between a first host which is not HIP enabled and a second host which is HIP enabled via a HIP proxy that avoids the above-mentioned problems.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention there is provided a method of at least partially securing communications, via a HIP proxy, between a first host which is not HIP enabled and a second host which is HIP enabled, the method comprising: sending a query from the first host to resolve the IP address of the second host; in response to said query, retrieving an IP address and HIT associated with the second host; in response to said retrieval, returning from the proxy a substitute IP address associated with the second host; maintaining at the proxy a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and upon receipt of a session initiation message at the proxy from the first host including as its destination address the substitute IP address, using the mapping to negotiate a HIP connection between the proxy and the second host.

The method may comprise looking up the retrieved IP address and the retrieved HIT from the mapping based on the substitute IP address in the session initiation message, and performing the HIP negotiation using the retrieved IP address and the retrieved HIT to locate and identify the Responder in the HIP negotiation together with an IP address and HIT of the proxy to locate and identify the Initiator in the HIP negotiation.

The retrieved IP address may be the IP address of a Forwarding Agent used by the second host, and further comprising initiating the HIP negotiation between the proxy and the second host by sending the initial HIP negotiation packet to the Forwarding Agent.

The method may further comprise, following receipt of the actual IP address of the second host at the proxy during the HIP negotiation, including the actual IP address in the mapping maintained at the proxy. The retrieved IP address may be replaced in the mapping by the actual IP address following its receipt at the proxy.

The retrieved IP address may be the actual IP address of the second host.

The method may comprise generating the substitute IP address at the proxy.

The method may further comprise, for an outgoing message received at the proxy after the HIP connection has been established including as its destination address the substitute IP address, using the mapping to route the message over the HIP connection to the second host. This may entail looking up the actual IP address and the retrieved HIT from the mapping based on the substitute IP address in the outgoing message, and routing the outgoing message to the second host using the actual IP address and the retrieved HIT to locate and identify the destination of the message, and using an IP address and HIT of the proxy to locate and identify the source of the message.

The method may further comprise completing the establishment of communications between the first and second hosts by forwarding the session initiation message from the proxy to the second host over the HIP connection, replying with a session acknowledgment message from the second host to the proxy over the HIP connection, and routing the session acknowledgment message to the first host. The session acknowledgment message may be a TCP ACK message.

The session initiation message may be a TCP SYN message.

The method may further comprise, for an incoming message received at the proxy from the second host over the established HIP connection, using a NAT function of the proxy to route the message to the appropriate destination host.

The above-mentioned query may be a DNS query. The proxy may intercept the DNS query from the first host. The proxy may perform the step of retrieving the IP address and HIT associated with the second host.

The proxy may retrieve the IP address and HIT associated with the second host from an external DNS server. Or the proxy may retrieve the IP address and HIT associated with the second host from an internal DNS server.

According to a second aspect of the present invention there is provided a communications system comprising a first host which is not HIP enabled, a second host which is HIP enabled, and a HIP proxy, wherein: the first host comprises means for sending a query to resolve the IP address of the second host; the proxy comprises means for retrieving, in response to said query, an IP address and HIT associated with the second host, for returning, in response to said retrieval, a substitute IP address associated with the second host, for maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT, and for using the mapping, upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, to negotiate a HIP connection between the proxy and the second host.

According to a third aspect of the present invention there is provided method for use by a HIP proxy of at least partially securing communications, via the proxy, between a first host which is not HIP enabled and a second host which is HIP enabled, the method comprising: receiving a query from the first host to resolve the IP address of the second host; in response to said query, retrieving an IP address and HIT associated with the second host; in response to said retrieval, returning a substitute IP address associated with the second host, and maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, using the mapping to negotiate a HIP connection between the proxy and the second host.

According to a fourth aspect of the present invention there is provided a HIP proxy for use in at least partially securing communications, via the proxy, between a first host which is not HIP enabled and a second host which is HIP enabled, comprising: means for receiving a query from the first host to resolve the IP address of the second host; means for retrieving, in response to said query, an IP address and HIT associated with the second host, for returning, in response to said retrieval, a substitute IP address associated with the second host, and maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and means for using the mapping, upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, to negotiate a HIP connection between the proxy and the second host.

According to a fifth aspect of the present invention there is provided a computer program which, when run on a HIP proxy, causes the proxy to carry out a method according to the third aspect of the present invention.

According to a sixth aspect of the present invention there is provided a computer program which, when loaded into a HIP proxy, causes the proxy to become one according to the fourth aspect of the present invention.

The computer program may be carried on a carrier medium, which may be a transmission medium or a storage medium.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1, discussed hereinbefore, illustrates the various layers in the Host Identity Protocol;

Figure 2, also discussed hereinbefore, illustrates the operation of the four-way handshake in the HIP protocol;

Figure 3, also discussed hereinbefore, shows the logical and actual packet structures in HIP;

Figure 4, also discussed hereinbefore, illustrates a hand over between IPv6 and IPv4;

Page 14a follows...

Figure 5, also discussed hereinbefore, is a schematic diagram illustrating the general network set up for communications between a legacy host and a HIP node via a HIP proxy;

Figure 6 is a message exchange diagram illustrating schematically a method of at least partially securing communications between a legacy host and a HIP host according to an embodiment of the present invention;

Page 15 follows...

WHAT IS CLAIMED IS:

1. A method of at least partially securing communications, via a Host Identity Protocol, HIP, proxy, between a first host which is not HIP enabled and a second host which is HIP enabled, the method comprising:

sending a query from the first host to resolve the Internet Protocol, IP, address of the second host;

in response to said query, retrieving an IP address and Host Identity Tag, HIT, associated with the second host;

in response to said retrieval, returning from the proxy a substitute IP address associated with the second host;

maintaining at the proxy a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and

upon receipt of a session initiation message at the proxy from the first host including as its destination address the substitute IP address, using the mapping to negotiate a HIP connection between the proxy and the second host.

2. A method as claimed in claim 1, comprising looking up the retrieved IP address and the retrieved HIT from the mapping based on the substitute IP address in the session initiation message, and performing the HIP negotiation using the retrieved IP address and the retrieved HIT to locate and identify the Responder in the HIP negotiation together with an IP address and HIT of the proxy to locate and identify the Initiator in the HIP negotiation.

3. A method as claimed in claim 1 or 2, wherein the retrieved IP address is the IP address of a Forwarding Agent used by the second host, and further comprising initiating the HIP negotiation between the proxy and the second host by sending the initial HIP negotiation packet to the Forwarding Agent.

4. A method as claimed in claim 3, further comprising, following receipt of the actual IP address of the second host at the proxy during the HIP negotiation, including the actual IP address in the mapping maintained at the proxy.

5. A method as claimed in claim 4, wherein the retrieved IP address is replaced in the mapping by the actual IP address following its receipt at the proxy.

6. A method as claimed in claim 1 or 2, wherein the retrieved IP address is the actual IP address of the second host.

7. A method as claimed in any preceding claim, comprising generating the substitute IP address at the proxy.

8. A method as claimed in any preceding claim, further comprising, for an outgoing message received at the proxy after the HIP connection has been established including as its destination address the substitute IP address, using the mapping to route the message over the HIP connection to the second host.

9. A method as claimed in claim 8, when dependent on claim 4, comprising looking up the actual IP address and the retrieved HIT from the mapping based on the substitute IP address in the outgoing message, and routing the outgoing message to the second host using the actual IP address and the retrieved HIT to locate and identify the destination of the message, and using an IP address and HIT of the proxy to locate and identify the source of the message.

10. A method as claimed in any preceding claim, further comprising completing the establishment of communications between the first and second hosts by forwarding the session initiation message from the proxy to the second host over the HIP connection, replying with a session acknowledgment message from the second host to the proxy over the HIP connection, and routing the session acknowledgment message to the first host.

11. A method as claimed in claim 10, wherein the session acknowledgment message is a TCP ACK message.

12. A method as claimed in any preceding claim, wherein the session initiation message is a TCP SYN message.

13. A method as claimed in any preceding claim, further comprising, for an incoming message received at the proxy from the second host over the established HIP connection, using a NAT function of the proxy to route the message to the appropriate destination host.

14. A method as claimed in any preceding claim, wherein the query is a DNS query.

15. A method as claimed in any preceding claim, wherein the proxy performs the step of retrieving the IP address and HIT associated with the second host.

16. A method as claimed in claim 15, wherein the proxy retrieves the IP address and HIT associated with the second host from an external DNS server.

17. A method as claimed in claim 15, wherein the proxy retrieves the IP address and HIT associated with the second host from an internal DNS server.

18. A method as claimed in any preceding claim, wherein the proxy intercepts the query from the first host.

19. A communications system comprising a first host which is not Host Identity Protocol, HIP, enabled, a second host which is HIP enabled, and a HIP proxy, wherein:

the first host comprises means for sending a query to resolve the Internet Protocol, IP, address of the second host;

the proxy comprises means for retrieving, in response to said query, an IP address and Host Identity Tag, HIT, associated with the second host, for returning, in response to said retrieval, a substitute IP address associated with the second host, for maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT, and for using the mapping, upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, to negotiate a HIP connection between the proxy and the second host.

20. A method for use by a Host Identity Protocol, HIP, proxy of at least partially securing communications, via the proxy, between a first host which is not HIP enabled

and a second host which is HIP enabled, the method comprising:

receiving a query from the first host to resolve the Internet Protocol, IP, address of the second host;

in response to said query, retrieving an IP address and Host Identity Tag, HIT, associated with the second host;

in response to said retrieval, returning a substitute IP address associated with the second host, and maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and

upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, using the mapping to negotiate a HIP connection between the proxy and the second host.

21. A Host Identity Protocol, HIP, proxy for use in at least partially securing communications, via the proxy, between a first host which is not HIP enabled and a second host which is HIP enabled, comprising:

means for receiving a query from the first host to resolve the Internet Protocol, IP, address of the second host;

means for retrieving, in response to said query, an IP address and Host Identity Tag, HIT, associated with the second host, for returning, in response to said retrieval, a substitute IP address associated with the second host, and maintaining a mapping between the substitute IP address, the retrieved IP address and the retrieved HIT; and

means for using the mapping, upon receipt of a session initiation message from the first host including as its destination address the substitute IP address, to negotiate a HIP connection between the proxy and the second host.

22. A computer program which, when run on a HIP proxy, causes the proxy to carry out a method as claimed in claim 20.

23. A computer program which, when loaded into a HIP proxy, causes the proxy to become one as claimed in claim 21.

24. A computer program as claimed in claim 22 or 23, carried on a carrier medium.

25. A computer program as claimed in claim 24, wherein the carrier medium is a transmission medium.

26. A computer program as claimed in claim 24, wherein the carrier medium is a storage medium.